THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

IN THE MATTER OF THE SEARCH OF: **ONE TARGET DEVICE IN THE UNITED STATES POSTAL INSPECTION SERVICE'S POSSESSION IN LINTHICUM HEIGHTS, MARYLAND**	**Misc. Case No.** 1:21-mj-320 TMD

AFFIDAVIT IN SUPPORT OF A SEARCH AND SEIZURE WARRANT

I, Douglas Henegar, being duly sworn, depose and state the following:

Introduction

1. Your Affiant makes this affidavit in support of an application under Federal Rule of Criminal Procedure 41 for a search and seizure warrant authorizing the examination of one cellular telephone, as fully described in Attachment A (collectively referred to as the "**TARGET DEVICE**"), and the extraction of electronically stored information identified in Attachment B from the **TARGET DEVICE**.

2. Your Affiant submits that probable cause exists to believe that (i) Barrington Albert Edwards, Jr. ("**EDWARDS**") engaged in drug trafficking activities in violation of 21 U.S.C. § 846; and (ii) the **TARGET DEVICE** contains fruits and evidence of drug trafficking activities, in violation of 21 U.S.C. §§ 841(a)(1), 843(b), and 846.

Affiant's Background

3. Your Affiant is "an investigative or law enforcement officer . . . of the United States" within the meaning of 18 U.S.C. § 2510(7)—that is, an officer of the United States of America ("United States") who is empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in 18 U.S.C. § 2516.

4. Your Affiant has been a United States Postal Inspector since April 2012 and is currently assigned to the United States Postal Inspection Service ("USPIS") Narcotics Team. As a United States Postal Inspector, your Affiant routinely investigates the use of the United States mail to ship narcotics and narcotics proceeds from source areas, such as Florida, Georgia, California, Arizona, Texas and Colorado, to the Baltimore/Washington, D.C. area and vice-versa.

5. In particular, your Affiant has participated in numerous drug trafficking investigations during which he conducted or participated in surveillance of drug dealers and others involved in drug trafficking; listened to hundreds of court-authorized intercepted phone calls between individuals involved or suspected to be involved in drug trafficking activities; made undercover purchases of drugs from drug dealers; applied for arrest and search warrants; executed arrest and search warrants; seized evidence relating to drug trafficking, including substantial quantities of narcotics, drug proceeds, and drug paraphernalia. In addition, your Affiant has worked directly with confidential informants and sources to conduct controlled drug purchases; debriefed them; and interviewed drug dealers and users about their lifestyles, appearances, and habits. Moreover, your Affiant has reviewed taped conversations, documents, and other records relating to drug trafficking and money laundering, including, but not limited to, buyers and sellers lists and owe sheets or drug ledgers.

6. Based on your Affiant's training and experience as a United States Postal Inspector, your Affiant can identify various methods that drug traffickers regularly use to facilitate the shipment of controlled substances and bulk cash through the United States mail. Specifically, your Affiant is aware that narcotic traffickers regularly use Priority Mail Express and Priority Mail services to ship controlled substances and bulk cash through the United States mail. Priority Mail Express labels have multi-layered carbon copies: The top copy with original writing is always

kept at the local post office; a second copy is given to the customer as a receipt; and a carbon copy stays on the parcel.

7. Prior to being a United States Postal Inspector, your Affiant was a United States Federal Air Marshall for ten (10) years. In that role, your Affiant primarily worked as a covert law enforcement officer protecting air craft passengers and infrastructure from terrorist threats as well as preventing the use of the airplane as a weapon of mass destruction.

8. Before his 10-year tenure as a United States Federal Air Marshall, your Affiant served a one-year stint as a United States Bureau of Customs and Border Protection patrol officer. In that capacity, your Affiant participated in alien-smuggling and drug interdictions at the southwest border of the United States.

9. Based on your Affiant's training, knowledge, and experience, he has become familiar with the following: (1) the manner in which drug traffickers (a) transport, store, and distribute drugs, (b) collect, keep, and conceal the proceeds of their illegal activities; and (2) the ways in which drug traffickers (a) use cellular telephones, cellular telephone technology, coded communications or slang during drug-related conversations, and (b) other means to facilitate their illegal activities and thwart law enforcement investigations.

10. Specifically, based on your Affiant's training, knowledge, and experience, your Affiant has learned the following:

a. Narcotics trafficking is an ongoing and recurring criminal activity. As contrasted with crimes against persons, which tend to be discrete offenses, narcotics trafficking is an illicit commercial activity that is characterized by regular, repeated criminal activity.

b. Narcotics traffickers commonly compartmentalize members of their organization into discrete "cells," with specific members, responsibilities, and/or geographical territories assigned to each cell, and members of one cell commonly receive information only about that specific cell's criminal

activities. Consequently, this limitation of information frustrates law enforcement efforts to dismantle the entire organization.

c. Cellular telephones are indispensable tools of the narcotics trafficking trade. Narcotics traffickers use cellular telephones, push-to-talk telephones, Short Message Service ("SMS"), electronic mail, and other, similar electronic means and/or devices to maintain contact with co-conspirators and other narcotics traffickers.

d. Narcotics traffickers commonly maintain books, records, receipts, notes, ledgers, bank records, money orders, and other papers relating to the importation, manufacture, transportation, ordering, sale, and distribution of narcotics. Narcotics traffickers maintain the aforementioned enumerated items where they have ready access to them, such as in secured locations within their residence, the residences of their friends, family members, and associates, or their drug distribution locations. Due to the advancement in technology, narcotics traffickers may use cellular telephones to store those records.

e. Narcotics traffickers usually take, or cause to be taken, photographs of themselves, their associates, their property, and illegal contraband. Drug traffickers usually maintain these photographs where they can readily access them, such as their cellular telephones.

f. Narcotics traffickers often use cellular telephones to maintain their co-conspirators' names and contact information, facilitate drug transactions, and run their drug distribution operations.

g. Drug trafficking organizations utilize the United States mail as a means of transporting narcotics and proceeds thereof to and from drug trafficking organization ("DTO") members. They use United States Priority Mail Express and Priority Mail services to ship narcotics and bulk-cash narcotics proceeds through the United States mail. Each United States Priority Mail Express and Priority Mail parcel has a distinct tracking number, and an individual with a tracking number can track the particular parcel online. Packages shipped to or from narcotics source states—such as Arizona, California, Texas, Washington, Colorado, and Florida—or territories—such as Puerto Rico—can signify that the United States Priority Mail Express and Priority Mail parcels contain narcotics or the proceeds thereof.

Bases of Information

11. The information contained in this affidavit is based upon my personal knowledge and observations as well as that of the other agents involved in this investigation. Those agents, persons with knowledge of this investigation, related those observations to me. Because I submit

this affidavit for the limited purpose of establishing probable cause for the requested search warrant, I have not included every fact and matter observed by or made known to agents of the government. Rather, I have set forth only those facts that I believe are necessary to establish probable cause.

Probable Cause

12. In early 2018, the United States Postal Inspection Service ("USPIS") and the Drug Enforcement Administration ("DEA") began jointly investigating the importation of large cocaine quantities from Puerto Rico to the United States. The USPIS identified certain United States Priority Mail parcels destined for different states, but they had the following similarities: addresses in heavy black magic marker, similar handwriting, no association between the senders' and recipients' names and their listed addresses, and Puerto Rico as the place the packages entered the mail stream. Among those United States Priority Mail parcels were the Florida Package, New York Package 1, and New York Package 2, and Postal Inspectors seized two cocaine bricks from the Florida Package, New York Package 1, and New York Package 2, weighing six kilograms in total.

13. There were also Priority Mail parcels destined for Bowie, Maryland, and Upper Marlboro, Maryland, with the aforementioned similarities (hereinafter "Subject Parcels"). As a result, investigators conducted surveillance in connection with the Subject Parcels' deliveries.

14. Among the DTO members that investigators identified based on physical surveillance, other law enforcement tools, and cellphone extractions were, (i) Russell Stanley III ("Stanley"), the DTO leader; (ii) **EDWARDS**, who worked closely with Stanley by serving as a liaison between Stanley and USPS letter carriers who **EDWARDS** recruited to—and did--divert United States Priority Mail parcels containing large quantities of cocaine to DTO members,

coordinating the delivery of cocaine parcels by a USPS letter carrier, directly paying or having others on his behalf paying a USPS letter carrier for diverting cocaine parcels to DTO members, and providing Stanley with addresses along the assigned postal route of a collusive USPS letter carrier; and (iii) Maurice Vaughn, a USPS letter carrier who diverted United States Priority Mail parcels containing large quantities of cocaine to DTO members.

15. During this investigation, there were at least 8 kilograms of cocaine intended for distribution seized during this conspiracy.

16. During the arrest of Stanley and other DTO members on October 9, 2019, investigators seized several cellular telephones. From one of those cellular telephones search pursuant to a federal search and seizure warrant, investigators extracted a text message exchange between Vaughn, via cellphone number ending in 1028, and **EDWARDS**, via a cellphone number ending in 8029, on January 19, 2020, beginning at approximately 9:00 a.m. Here is an excerpt of that text message exchange:

EDWARDS: Football should be in site.

VAUGHN: Looking for the game ball.

EDWARDS: Let me know. . . . Coach said football there.

VAUGHN: Yup found the ball.

EDWARDS: Good work tom. Time you running out tunnel with football. Want to catch an early Yo Brady.

Based on investigators' training, knowledge, and experience, including their experience in this investigation, investigators believe that, in vague, coded language, (1) **EDWARDS** informed Vaughn that the United States Priority Mail parcel containing cocaine should be among the mail that Vaughn would deliver along Vaughn's assigned route that day; (2) Vaughn told **EDWARDS** that Vaughn was checking to be sure; (3) **EDWARDS** asked Vaughn to confirm that Vaughn

possessed the cocaine parcel as Stanley told Edwards that the cocaine parcel should be there; (4) Vaughn confirmed that Vaughn found the cocaine parcel; and (5) **EDWARDS** indicated that he would like for Vaughn to divert the cocaine parcel to a DTO member earlier than their usual practice.

17. On October 21, 2020, a federal grand jury in the District of Maryland indicted, inter alia, the defendant Edwards with conspiracy to distribute and possess with the intent to distribute cocaine, in violation of 21 U.S.C. § 846; conspiracy to commit an offense against the United States, in violation of 18 U.S.C. § 371; and bribery, in violation of 18 U.S.C. § 201(b)(1). On the same day, Honorable J. Mark Coulson issued an arrest warrant for **EDWARDS**.

18. On January 6, 2021, investigators arrested **EDWARDS** in the District of New Jersey. Pursuant to a search incident to arrest, investigators seized the **TARGET DEVICE**.

Technical Terms

19. Based on my training and experience, your Affiant uses the following technical terms to convey the following meanings:

a. *Wireless telephone*: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include Global Positioning System ("GPS") technology for determining the location of the device.

b. *Digital camera*: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media includes various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. *Portable media player*: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media includes various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. *GPS*: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records of the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. *PDA*: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments, or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media includes various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA

users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include GPS technology for determining the location of the device.

f. *IP Address*: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

g. *Internet*: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

Based on your Affiant's training, experience, and research, he knows that the **TARGET DEVICE** has capabilities that allow them to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA, with the capability to access the Internet. In your Affiant's training and experience, examining data stored on a device of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the devices.

Electronic Storage and Forensic Analysis

20. Based on your Affiant's knowledge, training, and experience, he knows that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on such devices. This information can sometimes be recovered with forensics tools.

21. *Forensic evidence*. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the

TARGET DEVICE was used, the purpose of the **TARGET DEVICE**'s use, who used the **TARGET DEVICE**, and when was the **TARGET DEVICE** used. There is probable cause to believe that such forensic electronic evidence might be on the **TARGET DEVICE** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file).

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when were they used.

d. The process of identifying the exact electronically stored information on a storage medium that is necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when it was used, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

22. *Nature of examination*. Based on the foregoing, and consistent with Federal Rule of Criminal Procedure 41(e)(2)(B), the warrant for which the Affiant is applying would permit the examination of the **TARGET DEVICE** consistent with the warrant. The examination may require authorities to employ techniques, including, but not limited to, computer-assisted scans of the entire medium that might expose many parts of the **TARGET DEVICE** to human inspection in order to determine whether it is evidence described by the warrant.

23. *Manner of execution*. Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, your Affiant submits that there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

24. *Search and review protocol*: With respect to the search of the information provided pursuant to the requested warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored information that are identified with particularity in the requested warrant while minimizing the review of information not within the list of items to be seized as set forth in Attachment B, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.

Conclusion

25. Based on the foregoing, your Affiant respectfully submits that there is probable cause to believe that (i) **EDWARDS** engaged in drug trafficking activities in violation of 21 U.S.C. § 846; and (ii) a search of the **TARGET DEVICE**, in accord with Attachment B, will uncover evidence and fruits of drug trafficking activities, in violation of 21 U.S.C. §§ 841(a)(1), 843(b), and 846.

Respectfully submitted,

Douglas Henegar, Inspector
U.S. Postal Inspection Service

Affidavit submitted by e-mail and attested to me as accurate by telephone consistent with Fed. R. Crim. Proc. 4.1 and 41(d)(3) this 8 day of February, 2021

Honorable Thomas M. DiGirolamo
United States Magistrate Judge

Attachment A: TARGET DEVICE

The property to be searched is described as follows:

ITEM	DESCRIPTION	SEIZURE LOCATION
TARGET DEVICE	white Apple iPhone with silver trim	The person of Barrington Albert Edwards, Jr.

The **TARGET DEVICE** is in United States Postal Inspection Service's possession in Linthicum Heights, Maryland.

Attachment B: Items to Be Seized from the TARGET DEVICE

1. This warrant authorizes the search and seizure of all records contained within the devices described in Attachment A that constitute evidence of violations of 21 U.S.C. §§ 841(a)(1), 843(b), and 846 by Barrington Albert Edwards, Jr. and his known and unknown co-conspirators, including, but not limited to, the following:

a. images;

b. videos;

c. records of incoming and outgoing voice communications;

d. records of incoming and outgoing text messages;

e. the content of incoming and outgoing text messages;

f. voicemails;

g. e-mails;

h. voice recordings;

i. contact lists;

j. data from third-party applications (including social media applications like Facebook and Instagram and messaging programs like WhatsApp and Snapchat);

k. location data;

l. bank records, checks, credit card bills, account information, and other financial records;

m. evidence of who used, owned, or controlled the devices at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, "chat," instant messaging logs, photographs, and correspondence;

n. evidence of software that would allow others to control the **TARGET DEVICE**, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

o. evidence of the lack of such malicious software;

p. evidence of the attachment to the **TARGET DEVICE** of other storage devices or similar containers for electronic evidence;

q. evidence of counter forensic programs (and associated data) that are designed to eliminate data from the **TARGET DEVICE**;

r. evidence of the times the **TARGET DEVICE** was used;

s. passwords, encryption keys, and other access devices that may be necessary to access the **TARGET DEVICE**;

t. documentation and manuals that may be necessary to access the **TARGET DEVICE** or to conduct a forensic examination of the **TARGET DEVICE**; and

u. contextual information necessary to understand the evidence described in this attachment.

2. The search procedure of the electronic data for the items described in Paragraph 1 may include the following techniques (the following is a non-exhaustive list, and the Government may use other procedures that, like those listed below, minimize the review of information not within the list of items to be seized as set forth herein, while permitting the Government examination of all the data necessary to determine whether the data falls within the items to be seized):

a. surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for markings it contains and opening a drawer believed to contain pertinent files);

b. "opening" or cursorily reading the first few "pages" of such files in order to determine their precise contents;

c. "scanning" storage areas to discover and possible recover recently deleted files;

d. "scanning" storage areas for deliberately hidden files; or

e. performing key word or other search and retrieval searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are related to the subject matter of the investigation.

3. If after performing these procedures, the directories, files, or storage areas do not reveal evidence of violations of 21 U.S.C. §§ 841(a)(1) and 846, the further search of that particular directory, file, or storage area shall cease.

4. With respect to the search of the information provided pursuant to this warrant, law enforcement personnel will make reasonable efforts to use methods and procedures that will locate and expose those categories of files, documents, communications, or other electronically stored

information that are identified with particularity in the warrant while minimizing the review of information not within the list of items to be seized as set forth herein, to the extent reasonably practicable. If the government identifies any seized communications that may implicate the attorney-client privilege, law enforcement personnel will discontinue its review and take appropriate steps to segregate all potentially privileged information so as to protect it from substantive review. The investigative team will take no further steps regarding any review of information so segregated absent further order of the court. The investigative team may continue to review any information not segregated as potentially privileged.